(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－148593
（P2000－148593A）
(43)公開日　平成12年５月30日(2000.5.30)

(51)Int.Cl.'		識別記号	FI		テーマコード'（参考）
Ｇ０６Ｆ	12/14	３１０	Ｇ０６Ｆ 12/14	３１０Ｚ	
	12/16	３２０	12/16	３２０Ｂ	
	15/00	３３０	15/00	３３０Ａ	
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ 1/00	６４０Ｄ	
		６６０		６６０Ｅ	

審査請求　未請求　請求項の数12　ＯＬ　（全 20 頁）　最終頁に続く

(21)出願番号　特願平11－242712

(22)出願日　平成11年８月30日(1999.8.30)

(31)優先権主張番号　特願平10－244719
(32)優先日　平成10年８月31日(1998.8.31)
(33)優先権主張国　日本（ＪＰ）

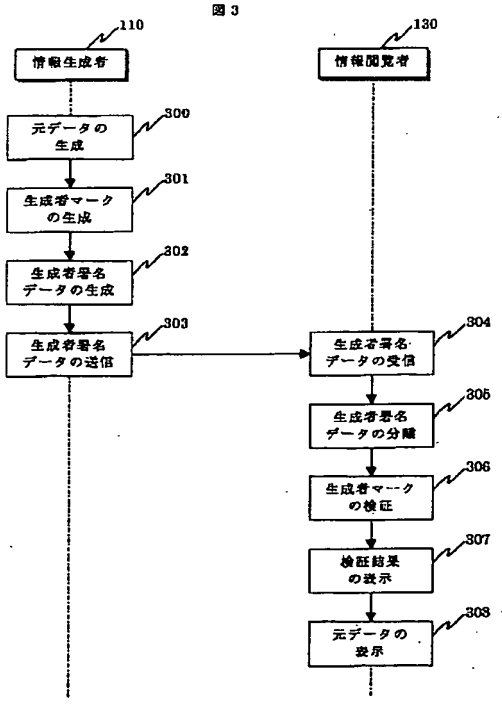
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　洲崎　誠一
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内
(72)発明者　豊島　久
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共情報事業部内
(74)代理人　100075096
弁理士　作田　康夫

最終頁に続く

(54)【発明の名称】　情報の認証システム

(57)【要約】
【課題】第一のユーザが生成したマルチメディアデータの真正性を，第二のユーザが視覚，聴覚などによって確認可能とする。
【解決手段】情報生成者１１０は，アプリケーションプログラムを使って情報閲覧者１３０に伝達する元データを生成する。次に，該元データの真正性を保証する生成者マークを生成し，当該元データと生成者マークとを一つに纏めて生成者署名データを生成する。そして，該生成者署名データを情報閲覧者１３０に送信する。生成者署名データを受け取った情報閲覧者１３０は，該生成者署名データを元データと生成者マークとに分離し，該生成者マークが確かに情報生成者１１０によって生成されたものであるか否かを検証する。そして，該検証結果を視覚，聴覚などによって確認するとともに，元データを適切なアプリケーションプログラムによって確認する。

図３



【特許請求の範囲】

【請求項１】情報生成用端末と，情報閲覧用端末と，が通信網を介して相互に接続されており，前記情報生成用端末は，前記情報閲覧用端末に伝達する第一のマルチメディアデータを生成する手段と，前記第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と，前記第一のマルチメディアデータと前記第二のマルチメディアデータとから第三のマルチメディアデータを生成し，該第三のマルチメディアデータを情報閲覧用端末に送付する手段と，を備え，前記情報閲覧用端末は，前記情報生成用端末から送付された前記第三のマルチメディアデータを受け取り，該第三のマルチメディアデータから，前記第一のマルチメディアデータと，前記第二のマルチメディアデータと，を分離する手段と，前記第二のマルチメディアデータを用いて，前記第一のマルチメディアデータの真正性を検証する手段と，前記第一のマルチメディアデータを閲覧可能とする手段と，を備えることを特徴とする情報の認証システム。

【請求項２】情報生成用端末と，情報閲覧用端末と，ゲートウェイ装置と，が通信網を介して相互に接続されており，前記情報生成用端末は，前記情報閲覧用端末に伝達する第一のマルチメディアデータを生成する手段と，前記第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と，前記第一のマルチメディアデータと前記第二のマルチメディアデータとから第三のマルチメディアデータを生成し，該第三のマルチメディアデータを，ゲートウェイ装置を介して情報閲覧用端末に送付する手段と，を備え，前記ゲートウェイ装置は，前記情報生成用端末から送付された前記第三のマルチメディアデータを受け取り，該第三のマルチメディアデータから，前記第一のマルチメディアデータと，前記第二のマルチメディアデータと，を分離する手段と，前記第二のマルチメディアデータを用いて，前記第一のマルチメディアデータの真正性を検証する手段と，前記第一のマルチメディアデータと，前記第二のマルチメディアデータと，真正性の検証処理の結果と，を情報閲覧用端末に送付する手段と，を備え，前記情報閲覧用端末は，前記ゲートウェイ装置から送付された前記第一のマルチメディアデータと，前記第二のマルチメディアデータと，真正性の検証処理の結果とを受け取り，該三種のデータを閲覧可能とする手段と，を備えることを特徴とする情報の認証システム。

【請求項３】情報生成用端末と，情報認証用端末と，情報閲覧用端末と，が通信網を介して相互に接続されており，前記情報生成用端末は，第一のマルチメディアデータを生成する手段と，前記第一のマルチメディアデータを前記情報認証用端末に送付する手段と，前記情報認証用端末から返送された第三のマルチメディアデータを受けとり，該第三のマルチメディアデータを前記情報閲覧用端末に送付する手段と，を備え，前記情報認証用端末は，前記情報生成用端末から送付された前記第一のマルチメディアデータを受け取り，該第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と，前記第一のマルチメディアデータと前記第二のマルチメディアデータとから第三のマルチメディアデータを生成し，該第三のマルチメディアデータを前記情報生成用端末に返送する手段と，を備え，前記閲覧用端末の端末は，前記情報生成用端末から送付された前記第三のマルチメディアデータを受け取り，該第三のマルチメディアデータから，前記第一のマルチメディアデータと，前記第二のマルチメディアデータと，を分離する手段と，前記第二のマルチメディアデータを用いて，前記第一のマルチメディアデータの真正性を検証する手段と，前記第一のマルチメディアデータを閲覧する手段と，を備えていることを特徴とする情報の認証システム。

【請求項４】情報生成用端末と，情報認証用端末と，情報閲覧用端末と，ゲートウェイ装置と，が通信網を介して相互に接続されており，前記情報生成用端末は，第一のマルチメディアデータを生成する手段と，前記第一のマルチメディアデータを前記情報認証用端末に送付する手段と，前記情報認証用端末から返送された第三のマルチメディアデータを受けとり，該第三のマルチメディアデータをゲートウェイ装置を介して前記情報閲覧用端末に送付する手段と，を備え，前記情報認証用端末は，前記情報生成用端末から送付された前記第一のマルチメディアデータを受け取り，該第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と，前記第一のマルチメディアデータと前記第二のマルチメディアデータとから第三のマルチメディアデータを生成し，該第三のマルチメディアデータを前記情報生成用端末に返送する手段と，を備え，前記ゲートウェイ装置は，前記情報生成用端末から送付された前記第三のマルチメディアデータを受け取り，該第三のマルチメディアデータから，前記第一のマルチメディアデータと，前記第二のマルチメディアデータと，を分離する手段と，前記第二のマルチメディアデータを用いて，前記第一のマルチメディアデータの真正性を検証する手段と，前記第一のマルチメディアデータと，前記第二のマルチメディアデータと，真正性の検証処理の結果と，を情報閲覧用端末に送付する手段と，を備え，前記情報閲覧用端末は，前記ゲートウェイ装置から送付された前記第一のマルチメディアデータと，前記第二のマルチメディアデータと，真正性の検証処理の結果とを受け取り，該三種のデータを閲覧可能とする手段と，を備えることを特徴とする情報の認証システム。

【請求項５】請求項１に記載された情報の認証システムであって，前記第二のマルチメディアデータを用いて，前記第一のマルチメディアデータの真正性を検証する手

段が，前記第二のマルチメディアデータの生成時に含めた，前記第一のマルチメディアデータの真正性を保証する証拠データを用いて行われるものであることを特徴とする情報の認証システム。

【請求項６】請求項１に記載された情報の認証システムであって，前記第一のマルチメディアデータの真正性を保証する前記第二のマルチメディアデータは，前記第一のマルチメディアデータまたはその圧縮子に対して施されたディジタル署名を含むことを特徴とする情報の認証システム。

【請求項７】請求項６記載の情報の認証システムであって，前記第一のマルチメディアデータの真正性を保証する前記第二のマルチメディアデータは，前記第一のマルチメディアデータまたはその圧縮子に対して施されたディジタル署名に加えて，該ディジタル署名を検証する際に使用する公開鍵，または電子認証書を含むことを特徴とする情報の認証システム。

【請求項８】請求項１に記載された情報の認証システムであって，前記第二のマルチメディアデータを用いて前記第一のマルチメディアデータの真正性を検証する手段は，視覚または聴覚によって確認できることを特徴とする情報の認証システム。

【請求項９】請求項１に記載された情報の認証システムであって，前記第二のマルチメディアデータを用いて前記第一のマルチメディアデータの真正性が確認された場合に，該第一のマルチメディアデータを閲覧可能にすることを特徴とする情報の認証システム。

【請求項１０】請求項３記載の情報の認証システムであって，前記情報生成用端末が、前記情報認証用端末に送付するデータは，前記第一のマルチメディアデータの圧縮子であることを特徴とする情報の認証システム。

【請求項１１】請求項６に記載された情報の認証システムであって，前記第二のマルチメディアデータを生成する場合に，前記第一のマルチメディアデータに関連する属性情報をもディジタル署名の対象とすることを特徴とする情報の認証システム。

【請求項１２】請求項１１記載の情報の認証システムであって，前記属性情報に，前記第一のマルチメディアデータに対するアクセス制御情報が含まれており，前記第一のマルチメディアデータの閲覧の可否を，該アクセス制御情報を用いて決定することを特徴とする情報の認証システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は，第一のユーザが生成した様々な種類のマルチメディアデータを，第二のユーザが入手・閲覧する情報システムにおいて，第二のユーザが当該マルチメディアデータの真正性を確認することができる認証システムに関する。

【０００２】

【従来の技術】パーソナルコンピュータのような情報機器の普及と通信ネットワークの整備に伴い，様々な情報が電子化され，ネットワークを介してやり取りされるようになってきている。このようなネットワークを介した情報のやり取りは，遠く離れた人とでも簡単，かつ高速に行うことができる反面，①通信データを第三者に盗聴される，②通信データを第三者に改ざんされる，③通信相手が自称する本人でない，などといった危険がある。

【０００３】これらの危険から情報システムを守るために，従来より暗号，認証などといったセキュリティ技術が広く用いられている。具体的には，前記第一の課題に対しては通信データを暗号化する。また，前記第二，第三の課題に対しては通信データにディジタル署名を付加する。

【０００４】このようなディジタル署名技術の概要については，例えば「Ｃｒｙｐｔｏｇｒａｐｈｙ ａｎｄ Ｄａｔａ Ｓｅｃｕｒｉｔｙ（著者：Ｄｏｒｏｔｈｙ Ｅｌｉｚａｂｅｔｈ Ｒｏｂｌｉｎｇ Ｄｅｎｎｉｎｇ，発行所：ＡＤＤＩＳＯＮ－ＷＥＳＬＥＹ ＰＵＢＬＩＳＨＩＮＧ ＣＯＭＰＡＮＹ）」の１４ページから１６ページに記載されている。

【０００５】ディジタル署名は，公開鍵暗号方式における暗号鍵の非対称性を利用した技術である。あるデータに対してディジタル署名を付加する方法，および，該ディジタル署名付きデータを検証する方法は，以下の通りである。

【０００６】データを生成した第一のユーザは，まず，生成したデータを自分の秘密鍵（第一のユーザが正しい値を知っている暗号鍵）で暗号化して暗号文（ディジタル署名）を生成する。次に元データとディジタル署名とを組にし，第二のユーザに渡す。第二のユーザは，ディジタル署名を上記第一のユーザの公開鍵（上記秘密鍵と一対一対応の関係にあり，第二のユーザも含めて，全てのユーザに対して正しい値が公開されている暗号鍵）で復号し，その結果と元データとを比較する。そして，復号結果と元データとが一致していた場合に，当該データを生成したのが第一のユーザ本人に間違いなく，かつ，当該データが改ざんされていないものと判断する。

【０００７】なぜなら，もし，不正を行おうとしている第三のユーザが生成したデータ，あるいは，該第三のユーザによって改ざんが加えられたデータであれば，ディジタル署名を第一のユーザの公開鍵で復号した結果と元データとが一致しないからである。言い換えれば，ディジタル署名を第一のユーザの公開鍵で復号した結果と元データが一致するということは，当該ディジタル署名を生成する際に，当該公開鍵を対応した第一のユーザの秘密鍵を用いたはずであり，第一のユーザの秘密鍵を用いることができるのは第一のユーザ本人だからである。

【０００８】上述のとおり，ディジタル署名技術を用いることにより，データの生成者は，当該データを生成し

たのが本人に間違いないこと，および当該データが改ざんされていないこと（本発明では，両性質をまとめて当該データの真正性と呼ぶ）を第三者に対して証明することができる。しかし，ディジタル署名自体は単なる数値データであり，その内容を人が見て直接解釈することは困難である。

【０００９】一方，多くの人は何かを見た場合に，そのものが示す意味までをも暗黙のうちに意識する。例えば，ブラウザプログラムを使って，インターネット上で公開された販売店のＷｅｂページを閲覧した場合に，もし，当該Ｗｅｂページに，あるクレジットカード会社のロゴマークが貼り付けられていたら，多くの閲覧者は当該販売店が当該クレジットカード会社の加盟店であり，その会社のクレジットカードで支払い処理を行うことができると判断することは容易に予想される。また，ワードプロセッサなどで生成された電子文書に，サインや印影などの画像データが貼付されていたら，当該サインや印影の対象者が当該データを生成した，あるいは当該データの内容を承認したと判断するものと考えられる。

【００１０】しかし，上記ロゴマークやサイン，印影などは単なる画像データであり，何ら証拠性（当該データが，貼付された画像データが意味する内容と合致していることに対する保証）を持つものではない。なぜなら，第一の情報（Ｗｅｂページや電子文書など）に貼付された画像データをコピーし，第二の情報に貼付することは，第一のデータの生成者だけでなく全ての人にとって容易だからである。

【００１１】そこで，ディジタル署名が正しく検証された場合に，サインや印影などの画像データを表示するように制御することで証拠性を保つ，ディジタル署名システムが考案されている。このようなディジタル署名システムについては，例えば米国特許５，６０６，６０９「ＥＬＥＣＴＯＲＯＮＩＣ　ＤＯＣＵＭＥＮＴ　ＶＥＲＩＦＩＣＡＴＩＯＮ　ＳＹＳＴＥＭ　ＡＮＤ　ＭＥＴＨＯＤ」に記載されている。

【００１２】

【発明が解決しようとする課題】ところで，現在の情報システムでは，様々な処理を電子的に行うために，テキストデータやワードプロセッサ文書，Ｗｅｂページ，図面，音声データ，画像データ，あるいはビデオデータなどといった多種多様なマルチメディアデータを取り扱うことが必要となっている。しかし，それらのマルチメディアデータは，それぞれ異なるデータ形式（データフォーマット）を有している。例えば，テキストデータはテキスト形式と呼ばれるデータフォーマットであり，Ｗｅｂページの多くはＨＴＭＬ形式と呼ばれるデータフォーマットである。さらに，画像データには，ビットマップ形式やＪＰＥＧ形式，ＧＩＦ形式などと呼ばれるいくつかのデータフォーマットを使うことが可能であり，ワードプロセッサ文書などは，それを処理するアプリケーションプログラム（ワードプロセッサ）独自のデータフォーマットを有している。

【００１３】現在の情報システムでは，上記データフォーマットの異なるマルチメディアデータを適切に処理するために様々なアプリケーションプログラムが併用されている。例えば，あるアプリケーションプログラムではテキストフォーマットのデータを処理し，別のアプリケーションプログラムでは，該アプリケーションプログラム独自のデータフォーマットのデータを処理している。また，さらに別のアプリケーションプログラムでは，複数種類のデータフォーマットのデータを処理することも可能である。

【００１４】このように，多種多様なデータフォーマットを有するマルチメディアデータを，多くのアプリケーションプログラムを使い分けることによって処理するような環境において，前記従来のディジタル署名技術を用いてデータの真正性を保証する場合，以下のような問題がある。

【００１５】上記環境において全てのマルチメディアデータの真正性を確認できるようにするためには，使用する全てのアプリケーションプログラムがディジタル署名を生成・検証するための機能を持たなければならない。しかし，現在，多くのアプリケーションプログラムはディジタル署名機能を有していない。そのため，たとえば，あるアプリケーションプログラムを用いて生成したマルチメディアデータにディジタル署名を付加した場合，新たに生成された署名付きマルチメディアデータのフォーマットは，元のマルチメディアデータのフォーマットとは異なるので，上記作成時に用いたアプリケーションプログラムでは処理できなくなってしまう。

【００１６】さらに，既存のアプリケーションプログラムにディジタル署名機能を追加するには，全てのアプリケーションプログラム開発者（開発企業）の協力が必要であり，実際にはきわめて困難である。

【００１７】また，前述のように，人は目で見たもの，あるいは音として聞いたものが示す意味を暗黙のうちに意識する傾向にある。したがって，単なるディジタル署名技術を適用するだけでなく，ディジタル署名の検証結果を視覚，聴覚などで直接的に確認できるようにしたほうが便利である。

【００１８】本発明は，上記事情に鑑みてなされたものであり，本発明の目的は，テキストデータやワードプロセッサ文書，Ｗｅｂページ，図面，音声データ，画像データ，あるいはビデオデータなどといったいくつかの異なるデータフォーマットを有するマルチメディアデータを取り扱う情報システムにおいて，該データフォーマットやそれらマルチメディアデータを処理するアプリケーションプログラムに依存することなく，第一のユーザが生成したマルチメディアデータの真正性を，第二のユーザが視覚，聴覚などで直接的に確認することができる認

証方法，およびそれを用いたシステム，さらには，該システムで使われる個々の装置と，それらを動作させるプログラムと，該システムに適したデータ構造を提供することである。

【００１９】

【課題を解決するための手段】上記課題を解決するために，本発明では，第一のユーザが生成した第一のマルチメディアデータと，視覚，聴覚で確認できる性質と真正性検証手段とを備えた第二のマルチメディアデータを組にして，第三のマルチメディアデータを生成し，第二のユーザは，第三のマルチメディアデータを第一のマルチメディアデータと第二のマルチメディアデータとに分離した後，第二のマルチメディアデータが備える，視覚，聴覚で確認できる性質と真正性検証手段とを用いて，第一のマルチメディアデータが真正なものであるか否かを，視覚，聴覚によって確認するとともに，第一のマルチメディアデータを適切なアプリケーションプログラムを用いて処理することを特徴とする。

【００２０】本発明によれば，まず，第一のユーザが任意のアプリケーションプログラムを用いて生成した第一のマルチメディアデータが真正なものであるか否かという証拠，すなわち，第二のマルチメディアデータを，第一のユーザ，あるいは全てのユーザが信頼する第三者（第三者機関）が生成したのち，該第一，第二のマルチメディアデータを組にして第三のマルチメディアデータを生成するようにしている。さらに，第二のユーザは，第三のマルチメディアデータを第一のマルチメディアデータと第二のマルチメディアデータとに分離した後，第二のマルチメディアデータが有する，視覚，聴覚で確認できる性質と真正性検証手段とを用いて第一のマルチメディアデータの真正性を視覚，聴覚で確認するようにしている。加えて，第一のマルチメディアデータを適切なアプリケーションプログラム，すなわち，第二のユーザが使用可能なアプリケーションプログラムの中で，第一のマルチメディアデータのデータフォーマットを処理可能なアプリケーションプログラムを用いて，該第一のマルチメディアデータを処理するようにしている。

【００２１】すなわち，本発明の情報の認証システムは，情報生成用端末と，情報閲覧用端末と，が通信網を介して相互に接続されており，情報生成用端末は，情報閲覧用端末に伝達する第一のマルチメディアデータを生成する手段と，第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と，第一のマルチメディアデータと第二のマルチメディアデータとから第三のマルチメディアデータを生成し，該第三のマルチメディアデータを情報閲覧用端末に送付する手段とを備え，情報閲覧用端末は，情報生成用端末から送付された第三のマルチメディアデータを受け取り，該第三のマルチメディアデータから，第一のマルチメディアデータと，第二のマルチメディアデータとを分離する手段と，第二のマルチメディアデータを用いて，第一のマルチメディアデータの真正性を検証する手段と，第一のマルチメディアデータを閲覧可能とする手段とを備えることを特徴としている。

【００２２】また，本発明の情報の認証システムは，情報生成用端末と，情報閲覧用端末と，ゲートウェイ装置と，が通信網を介して相互に接続されており，情報生成用端末は，情報閲覧用端末に伝達する第一のマルチメディアデータを生成する手段と，第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と，第一のマルチメディアデータと第二のマルチメディアデータとから第三のマルチメディアデータを生成し，該第三のマルチメディアデータを，ゲートウェイ装置を介して情報閲覧用端末に送付する手段とを備え，ゲートウェイ装置は，情報生成用端末から送付された第三のマルチメディアデータを受け取り，該第三のマルチメディアデータから，第一のマルチメディアデータと，第二のマルチメディアデータとを分離する手段と，第二のマルチメディアデータを用いて，第一のマルチメディアデータの真正性を検証する手段と，第一のマルチメディアデータと，第二のマルチメディアデータと，真正性の検証処理の結果とを情報閲覧用端末に送付する手段とを備え，情報閲覧用端末は，ゲートウェイ装置から送付された第一のマルチメディアデータと，第二のマルチメディアデータと，真正性の検証処理の結果とを受け取り，該三種のデータを閲覧可能とする手段とを備えることを特徴としている。

【００２３】また，本発明の情報の認証システムは，情報生成用端末と，情報認証用端末と，情報閲覧用端末と，が通信網を介して相互に接続されており，情報生成用端末は，第一のマルチメディアデータを生成する手段と，第一のマルチメディアデータを情報認証用端末に送付する手段と，情報認証用端末から返送された第三のマルチメディアデータを受けとり，該第三のマルチメディアデータを情報閲覧用端末に送付する手段とを備え，情報認証用端末は，情報生成用端末から送付された第一のマルチメディアデータを受け取り，該第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と，第一のマルチメディアデータと第二のマルチメディアデータとから第三のマルチメディアデータを生成し，該第三のマルチメディアデータを情報生成用端末に返送する手段とを備え，閲覧用端末の端末は，情報生成用端末から送付された第三のマルチメディアデータを受け取り，該第三のマルチメディアデータから，第一のマルチメディアデータと，第二のマルチメディアデータとを分離する手段と，第二のマルチメディアデータを用いて，第一のマルチメディアデータの真正性を検証する手段と，第一のマルチメディアデータを閲覧する手段とを備えていることを特徴としている。

【００２４】また，本発明の情報の認証システムは，情

報生成用端末と，情報認証用端末と，情報閲覧用端末と，ゲートウェイ装置と，が通信網を介して相互に接続されており，情報生成用端末は，第一のマルチメディアデータを生成する手段と，第一のマルチメディアデータを情報認証用端末に送付する手段と，情報認証用端末から返送された第三のマルチメディアデータを受けとり，該第三のマルチメディアデータをゲートウェイ装置を介して情報閲覧用端末に送付する手段とを備え，情報認証用端末は，情報生成用端末から送付された第一のマルチメディアデータを受け取り，該第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成する手段と，第一のマルチメディアデータと第二のマルチメディアデータとから第三のマルチメディアデータを生成し，該第三のマルチメディアデータを情報生成用端末に返送する手段とを備え，ゲートウェイ装置は，情報生成用端末から送付された第三のマルチメディアデータを受け取り，該第三のマルチメディアデータから，第一のマルチメディアデータと，第二のマルチメディアデータとを分離する手段と，第二のマルチメディアデータを用いて，第一のマルチメディアデータの真正性を検証する手段と，第一のマルチメディアデータと，第二のマルチメディアデータと，真正性の検証処理の結果とを情報閲覧用端末に送付する手段とを備え，情報閲覧用端末は，ゲートウェイ装置から送付された第一のマルチメディアデータと，第二のマルチメディアデータと，真正性の検証処理の結果とを受け取り，該三種のデータを閲覧可能とする手段とを備えることを特徴としている。

【００２５】さらに，本発明の情報の認証システムは，第二のマルチメディアデータを用いて，第一のマルチメディアデータの真正性を検証する手段が，第二のマルチメディアデータの生成時に含めた，第一のマルチメディアデータの真正性を保証する証拠データを用いて行われるものであることを特徴としている。

【００２６】さらに，本発明の情報の認証システムは，第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータは，第一のマルチメディアデータまたはその圧縮子に対して施されたディジタル署名を含むことを特徴としている。

【００２７】さらに，本発明の情報の認証システムは，第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータは，第一のマルチメディアデータまたはその圧縮子に対して施されたディジタル署名に加えて，該ディジタル署名を検証する際に使用する公開鍵，または電子認証書を含むことを特徴としている。

【００２８】さらに，本発明の情報の認証システムは，第二のマルチメディアデータを用いて第一のマルチメディアデータの真正性を検証する手段は，視覚または聴覚によって確認できることを特徴としている。

【００２９】さらに，本発明の情報の認証システムは，第二のマルチメディアデータを用いて第一のマルチメディアデータの真正性が確認された場合に，該第一のマルチメディアデータを閲覧可能にすることを特徴としている。

【００３０】さらに，本発明の情報の認証システムは，情報生成用端末が，情報認証用端末に送付するデータは，第一のマルチメディアデータの圧縮子であることを特徴としている。

【００３１】さらに，本発明の情報の認証システムは，第二のマルチメディアデータを生成する場合に，第一のマルチメディアデータに関連する属性情報をもディジタル署名の対象とすることを特徴としている。

【００３２】さらに，本発明の情報の認証システムは，属性情報に，第一のマルチメディアデータに対するアクセス制御情報が含まれており，第一のマルチメディアデータの閲覧の可否を，該アクセス制御情報を用いて決定することを特徴としている。

【００３３】また，本発明による真正性保証プログラムは，真正性保証データの生成指示を受けた場合に，第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータを生成した後，該第一のマルチメディアデータと該第二のマルチメディアデータとから第三のマルチメディアデータを生成する手段，または，真正性保証データの検証指示を受けた場合に，受け取った第三のマルチメディアデータを，第一のマルチメディアデータと第二のマルチメディアデータとに分離した後，該第二のマルチメディアデータの真正性検証手段を用いて，該第一のマルチメディアデータの真正性を検証するとともに，視覚または，聴覚によって確認可能な方法により該検証結果を出力する手段を備えることを特徴としている。

【００３４】また，本発明による真正性保証プログラムは，第三のマルチメディアデータの生成は，第一のマルチメディアデータと第二のマルチメディアデータに関する情報に基づいてヘッダ情報を生成した後，該ヘッダ情報と第一と第二のマルチメディアデータとを結合することによって行い，第三のマルチメディアデータの分離は，ヘッダ情報に基づいて第一のマルチメディアデータと第二のマルチメディアデータとを抽出することによって行うことを特徴としている。

【００３５】さらに，本発明による真正性保証プログラムは，第三のマルチメディアデータの生成は，第一のマルチメディアデータに第二のマルチメディアデータに対するリンク情報を示すタグを追加することによって行ない，第三のマルチメディアデータの分離は，リンク情報を抽出することによって行うことを特徴としている。

【００３６】さらに，本発明による真正性保証プログラムは，該真正性保証プログラムが動作する端末において，第一のマルチメディアデータを処理可能なアプリケーションプログラムが存在した場合には，該アプリケーションプログラムに第一のマルチメディアデータを渡し

て，該アプリケーションプログラムを起動することを特徴としている。

【００３７】さらに，本発明による真正性保証プログラムは，真正性保証データの検証を開始する際の指示が第三のマルチメディアデータを受け取ることであることを特徴としている。

【００３８】さらに，本発明による真正性保証プログラムは，真正性保証データの検証を開始する際の指示が閲覧用端末の利用者からによる明示的な命令であることを特徴としている。

【００３９】また，本発明によるマルチメディアデータは，情報生成用端末が生成した第一のマルチメディアデータと，第一のマルチメディアデータの真正性を保証する第二のマルチメディアデータと，第一のマルチメディアデータと第二のマルチメディアデータとを分離するために必要な属性情報と，からなることを特徴としている。

【００４０】さらに，本発明によるマルチメディアデータは，第二のマルチメディアデータに対するリンク情報を示すタグが，該第二のマルチメディアデータに証拠データが含まれることを明示的に示すものであることを特徴としている。

【００４１】したがって，本発明によれば，第一のマルチメディアデータのデータフォーマットや，第一のマルチメディアデータを生成する際に第一のユーザが使用したアプリケーションプログラムに依存することなく，第二のユーザが，第二のマルチメディアデータの真正性検証手段を用いて，第一のマルチメディアデータの真正性を視覚，聴覚などで正しく確認することができる。

【００４２】

【発明の実施の形態】以下，図面を用いて，本発明の実施例を説明する。なお，以下で説明する図面において，同一の番号は同様の部品・要素を表すものとする。また，これにより本発明が限定されるものではない。

【００４３】図１は，本発明の第一の実施形態が適用された認証システムの概略構成を示す図である。本実施形態の認証システムは，各種マルチメディアデータ（前述の第一のマルチメディアデータ，以下，単に元データと称する）を生成する情報生成者１１０と，元データの真正性を保証するマルチメディアデータ（情報認証者１１０が生成する前述の第二のマルチメディアデータ，以下，単に認証者マークと称する）を発行する情報認証者１２０と，情報生成者１１０が生成した元データを閲覧する情報閲覧者１３０とが利用するシステムであって，図１に示すように，端末１４０_{1}～１４０_{3}（以下，単に端末１４０とも称する）が通信網１００を介して，互いに接続された構成になっている。

【００４４】端末１４０_{1}は，情報生成者１１０が使用する端末である。情報生成者１１０は，端末１４０_{1}を使って，元データを生成したり，元データの真正性を保証するマルチメディアデータ（情報生成者１１０が生成する前述の第二のマルチメディアデータ，以下，単に生成者マークと称する）を生成したり，元データと生成者マークとから，前述の第三のマルチメディアデータ（以下，単に生成者署名データと称する）を生成したりする。さらに，通信網１００を介して，情報認証者１２０や情報閲覧者１３０とデータのやり取りを行う。

【００４５】なお、本明細書を実現する場合の生成者マークのデータ形式は限定されず、人間が見ることができて，かつ，データを埋め込むことができるものであればよい。具体的には、BMP、JPEGなど既存のデータ形式を使用することが可能である。また、静止画、動画、さらには、複数枚の静止画を順番に切り替え表示するデータ形式であってもよい。

【００４６】端末１４０_{2}は，情報認証者１２０が使用する端末である。情報認証者１２０は，端末１４０_{2}を使って，情報生成者１１０が生成した元データに対する認証者マークを生成したり，元データと認証者マークとから，前述の第三のマルチメディアデータ（以下，単に認証者署名データと称する）を生成したりする。さらに，通信網１００を介して，情報生成者１１０とデータのやり取りも行う。上記元データと認証者マークとから第三のマルチメディアデータを生成する方法については後述する。

【００４７】端末１４０_{3}は，情報閲覧者１３０が使用する端末である。端末１４０_{3}は，情報閲覧者１３０に，文書データや画像データなどを表示する表示装置１４１と，情報閲覧者１３０がデータや命令などを入力するための入力装置１４２_{1}や１４２_{2}（以下，単に入力装置１４２とも称する）を備えている。情報閲覧者１３０は，端末１４０_{3}を使って，生成者署名データ（または，認証者署名データ）を，生成者マーク（または，認証者マーク）と元データとに分離したり，生成者マーク（または，認証者マーク）を検証したり，元データを閲覧したりする。さらに，通信網１００を介して，情報生成者１１０とデータのやり取りを行う。上記生成者署名データ（または，認証者署名データ）を生成者マーク（または，認証者マーク）と元データとに分離する方法については後述する。

【００４８】次に，本実施形態の認証システムを構成する端末１４０を図面を参照して詳細に説明する。

【００４９】図２は，端末１４０のハードウェア構成を示す図である。

【００５０】本実施形態の端末１４０のハードウェア構成は，図２に示すように，表示装置１４１と，入力装置１４２と，通信網インタフェース２０１と，記憶装置２０２と，中央処理装置（ＣＰＵ）２０３と，一時記憶装置（メモリ）２０４とが，バス２００によって互いに接続されて構成されている。

【００５１】表示装置１４１は，端末１４０を使用する

情報生成者１１０，情報認証者１２０，あるいは情報閲覧者１３０（以下，全てを纏めて単に利用者とも称する）に各種データを表示するために用いられるものであり，ＣＲＴや液晶ディスプレイなどで構成される。

【００５２】入力装置１４２は，端末１４０を使用する利用者がデータや命令などを入力するために用いられるものであり，キーボードやマウスなどで構成される。

【００５３】通信網インターフェース２０１は，通信網１００を介して他の端末とデータのやり取りを行うためのインタフェースである。

【００５４】記憶装置２０２は，端末１４０で使用されるプログラムやデータを永続的に記憶するために用いられるものであり，ハードディスクやフロッピーディスクなどで構成される。

【００５５】ＣＰＵ２０３は，端末１４０を構成する各部を統括的に制御したり，様々な演算処理を行ったりする。

【００５６】メモリ２０４には，オペレーティングシステム２０４ａ（以下，単にＯＳ２０４ａとも称する）や，アプリケーションプログラム２０４ｂ，あるいは真正性保証プログラム２０４ｃなどといった，ＣＰＵ２０３が上記の処理をするために必要なプログラムなどが一時的に格納される。

【００５７】ＯＳ２０４ａは，端末１４０全体の制御を行うために，ファイル管理やプロセス管理，あるいはデバイス管理といった機能を実現するためのプログラムである。

【００５８】アプリケーションプログラム２０４ｂは，元データを生成，閲覧したり，通信網１００を介して他の端末とデータのやり取りを行ったりするためのプログラム群である。

【００５９】真正性保証プログラム２０４ｃは，生成者マーク（または，認証者マーク）を生成するためや，生成者マーク（または，認証者マーク）と元データとから，生成者署名データ（または，認証者署名データ）を生成するためや，生成者マーク（または，認証者マーク）を検証してその結果を表示するためのプログラムである。すなわち，情報生成者１１０は，該真正性保証プログラム２０４ｃを使って，生成者マークと生成者署名データとを生成する。また，情報認証者１２０は，該真正性保証プログラム２０４ｃを使って，認証者マークと認証者署名データとを生成する。さらに，情報閲覧者１３０は，該真正性保証プログラム２０４ｃを使って，生成者署名データ（認証者署名データ）から生成者マーク（認証者マーク）を分離した後，該生成者マーク（認証者マーク）を用いて元データの真正性を検証するとともに，その結果を表示する。

【００６０】端末１４０_1ないし１４０_3上で動作するアプリケーションプログラム２０４ｂと真正性保証プログラム２０４ｃは，上記すべての処理を行なえるものでなくても良く，同じマルチメディアデータを扱えるものであって，自端末に必要な処理を行なえるものであればよい。また，端末１４０_1ないし１４０_3は，同一でなくても良く，それぞれの端末に必要な機能を持っていればよい。

【００６１】また、以下の説明で各アプリケーションプログラム、真正性保証プログラム２０４ｃの各動作はオペレーティングシステムの制御の元で行われることもある。

【００６２】次に，本実施形態の認証システムの動作について説明する。

【００６３】図３は，情報生成者１１０が生成した元データの真正性を，情報閲覧者１３０が生成者署名データを用いて検証する場合の，情報生成者１１０と情報閲覧者１３０の動作を説明するための図である。

【００６４】図３において，情報生成者１１０が行う処理には端末１４０_1が使用され，情報閲覧者１３０が行う処理には端末１４０_3が使用される。

【００６５】まず，情報生成者１１０は，情報閲覧者１３０に伝達する元データを生成する（ステップ３００）。次に，該元データの真正性を保証する生成者マークを生成し（ステップ３０１），当該元データと生成者マークとから生成者署名データを生成する（ステップ３０２）。そして，該生成者署名データを情報閲覧者１３０に送信する（ステップ３０３）。上記情報生成者１１０の処理の詳細については，後ほど，図４を用いて説明する。

【００６６】生成者署名データを受け取った情報閲覧者１３０は（ステップ３０４），まず，該生成者署名データを元データと生成者マークとに分離し（ステップ３０５），該生成者マークが確かに情報生成者１１０によって生成されたものであるか否かを検証する（ステップ３０６）。そして，該検証結果を確認するとともに（ステップ３０７），元データを確認し（ステップ３０８），全ての処理を終了する。上記情報閲覧者１３０の処理の詳細については，後ほど，図５を用いて説明する。

【００６７】上記手順において，情報閲覧者１３０による真正性の確認は，たとえば，図１に示すように表示装置１４１に「本物です」（あるいは「にせものです」，「生成者マークではありません」）といった吹き出しが表示され，情報閲覧者１３０が該吹き出しを見ることによって行われる。しかし，本発明自体は，上記表示方法に限定されるものでなく別の表示方法を用いてもよい。たとえば，メッセージボックスやダイアログボックスなどで表示してもよい。また，音などを用いて行ってもよいし，音，表示を組み合わせてもよい。

【００６８】さらに，上記手順における，情報生成者１１０が情報閲覧者１３０に対して生成者署名データを送る際の，送信手段は，本発明では限定しない。オンライン（たとえば，電子メールなど）であってもオフライン

（たとえば，フロッピーディスクの郵送など）であってもよい。また，たとえば，情報生成者１１０がＷｅｂサーバを使って公開している生成者署名データを，情報閲覧者１３０がブラウザプログラムを使って自発的に取りにいくようにしてもよい。

【００６９】図４は，図３における情報生成者１１０側の処理の詳細を示す図である。

【００７０】図４において，一重枠と二重枠とは，それぞれデータとプログラム処理とを表している。

【００７１】情報生成者１１０側の処理は，元データ４００を生成するアプリケーションプログラム（マルチメディアデータ処理プログラム）２０４ｂ１と，該元データ４００に対応する生成者署名データ４０７を生成する真正性保証プログラム２０４ｃと，該生成者署名データ４０７を情報閲覧者に渡すアプリケーションプログラム（通信プログラム）２０４ｂ２とが連携して行う。図４に示すように，本実施例では，アプリケーションプログラム２０４ｂ１と２０４ｂ２，および真正性保証プログラム２０４ｃとを，それぞれ異なる機能を具備するプログラムとして記載している。しかし，本発明自体は，上記形態に限定されるものではない。たとえば，アプリケーションプログラム２０４ｂ１とアプリケーションプログラム２０４ｂ２とが一つのプログラムであってもよい。また，真正性保証プログラム２０４ｃが，アプリケーションプログラム２０４ｂ１のアドイン（プラグイン）プログラムまたは，マクロプログラムであってもよい。

【００７２】まず，アプリケーションプログラム２０４ｂ１は，生成した（元データの生成３００）元データ４００を，真正性保証プログラム２０４ｃに渡す。該二つのプログラム間での元データ４００の受け渡し方法としては，アプリケーションプログラム２０４ｂ１が元データ４００をファイルとして記憶装置に書き込み，真正性保証プログラム２０４ｃが該記憶装置から読み取るといった方法が考えられる。しかし，本発明自体は，上記方法に限定されるものではなく，メモリを介して受け渡してもよい。

【００７３】次に，真正性保証プログラム２０４ｃは，該元データ４００を所定の圧縮関数を使って圧縮して圧縮子４０１を生成した後，該圧縮子４０１に対して情報生成者１１０の秘密鍵４０２を使ってディジタル署名処理４０３を施し，元データ４００に対する情報生成者１１０のディジタル署名４０４を生成する。上記手順のように，元データ４００に直接ディジタル署名を施すのではなく，その圧縮子４０１に対してディジタル署名を施すという手法は，ディジタル署名処理にかかる時間を減らすために一般的に行われているものである。しかし，本発明自体は，上記処理方法に限定されるものでなく，元データ４００に対して直接ディジタル署名を施すようにしてもよい。

【００７４】なお、上記圧縮関数には，たとえば、ハッシュ関数のような不可逆性ものでも良いし，可逆性のものでも良い。

【００７５】次に，真正性保証プログラム２０４ｃは，上記情報生成者１１０のディジタル署名４０４と画像データ４０５とから，生成者マーク４０６を生成する（生成者マークの生成３０１）。上記画像データ４０５は，情報閲覧者１３０の表示装置１４１において検証結果表示時に表示されるものであり，たとえば，ロゴマークや印影のようなものである。なお，上記画像データ４０５の生成は，画像データを処理可能なアプリケーションプログラムを用いて別途行っておく。上記ディジタル署名４０４と画像データ４０５とを一纏めにする手法としては，たとえば，「ＩＢＭ　ＳＹＳＴＥＭＳ　ＪＯＵＲＮＡＬ，ＶＯＬ３５，ＮＯＳ３＆４，１９９６」の３１３ページから３３６ページに記載されているような電子透かし技術の利用が可能である。電子透かしは，画像データに微少な変更を加えることで，情報を埋め込む技術である。本発明において，ディジタル署名４０４と画像データ４０５とを一纏めにする手段として電子透かしを用いる場合，画像データの視認性（人がその画像データを見て感じ取る情報）さえ阻害しなければ，画像データ自体は多少変形されてもよい。しかし，本発明自体は，上記手法に限定されるものでなく別の手法、例えばハイパーリンクのような関連づけの方法を用いてもよい。

【００７６】次に，真正性保証プログラム２０４ｃは，上記生成者マーク４０６と元データ４００とから生成者署名データ４０７を生成する（生成者署名データの生成３０２）。生成者署名データ４０７を生成する手法としては，たとえば，図７に示すように，ヘッダ情報を付して二つのマルチメディアデータを単純に結合して，生成者署名データ用フォーマットに変換し，さらにデータ名の一部である拡張子を変換する方法がある。ヘッダ情報とは，真正性保証プログラム２０４ｃによって生成される属性情報であり，上記二つのデータをあとで正しく分離するために必要な，該二つのデータの大きさや元々のファイル名などを含んでいる。図７において真正性保証プログラム２０４ｃが生成者署名データ４０７を生成する際の処理の流れを図１１に示す。

【００７７】図１１において，真正性保証プログラム２０４ｃは，まず，元データに関する情報と生成者マークに関する情報とを調べ（ステップ１１００，１１０１），該情報に基づいてヘッダ情報を生成する（ステップ１１０２）。そして，該ヘッダ情報と元データ，および生成者マークを結合して生成者署名データを生成する（ステップ１１０３）。上記手順において，三つのデータの結合は，たとえば，ヘッダ情報の最後尾に元データの先頭を連結し，さらに，該元データの最後尾に生成者マークの先頭を連結するような方法で行う。

【００７８】また，生成者マーク４０６と元データ４０

０とを一纏めにする際に，上記図７に示すように生成者署名データ用フォーマットに変換して一つのデータにするのではなく，図８に示すように，タグなどリンク情報を用いて元データと生成者マークとを単に関連付けるだけでもよい。ただし，本発明自体は，上記二つの手法に限定されるものでなく別の方法を用いてもよい。

【００７９】再び，図４を参照して情報生成者１１０側の処理の詳細を説明する。

【００８０】真正性保証プログラム２０４ｃは，上記生成者署名データ４０７を生成したら，次に，該生成者署名データ４０７をアプリケーションプログラム２０４ｂ２に渡す。該二つのプログラム間での生成者署名データ４０７の受け渡し方法としては，真正性保証プログラム２０４ｃが生成者署名データ４０７をファイルとして記憶装置に書き込み，アプリケーションプログラム２０４ｂ２が該記憶装置から読み取るといった方法が考えられる。しかし，本発明自体は，上記方法に限定されるものではなく，メモリを介して受け渡してもよい。もちろん，真正性保証プログラム２０４ｃは，該生成者署名データ４０７をアプリケーションプログラム２０４ｂ１に戻しても良い。

【００８１】最後に，アプリケーションプログラム２０４ｂ２は，生成者署名データ４０７を情報閲覧者１３０に送信する（生成者署名データの送信３０３）。

【００８２】図５は，図３における情報閲覧者１３０側の処理の詳細を示す図である。

【００８３】図５において，一重枠と二重枠とは，それぞれデータとプログラム処理とを表している。

【００８４】情報閲覧者１３０側の処理は，生成者署名データ４０７を受け取るアプリケーションプログラム（通信プログラム）２０４ｂ２と，該生成者署名データ４０７を用いて元データ４００の真正性を検証する真正性保証プログラム２０４ｃと，元データ４００を表示するアプリケーションプログラム（マルチメディアデータ処理プログラム）２０４ｂ１とが連携して行う。図５に示すように，本実施例では，アプリケーションプログラム２０４ｂ１と２０４ｂ２，および真正性保証プログラム２０４ｃとを，それぞれ異なる機能を具備するプログラムとして別々に記載している。しかし，本発明自体は，上記形態に限定されるものではない。たとえば，アプリケーションプログラム２０４ｂ１とアプリケーションプログラム２０４ｂ２とが一つのプログラムであってもよい。また，真正性保証プログラム２０４ｃが，アプリケーションプログラム２０４ｂ１のアドイン（プラグイン）プログラムやマクロプログラムであってもよい。

【００８５】まず，アプリケーションプログラム２０４ｂ２は，生成者署名データ４０７を受け取り（生成者署名データの受信３０４），該生成者署名データ４０７を真正性保証プログラム２０４ｃに渡す。該二つのプログラム間での生成者署名データ４０７の受け渡し方法としては，アプリケーションプログラム２０４ｂ２が生成者署名データ４０７をファイルとして記憶装置に書き込み，真正性保証プログラム２０４ｃが該記憶装置から読み取るといった方法が考えられる。しかし，本発明自体は，上記方法に限定されるものではなく，メモリを介して受け渡してもよい。

【００８６】ところで，上記処理手順において，生成者署名データ４０７が前記図７に示すような方法によって一つのデータに纏められている場合，アプリケーションプログラム２０４ｂ２（情報閲覧者１３０）は，受け取ったデータ名の拡張子を調べることによって，当該データが生成者署名データ４０７であると判断することができる。一方，生成者署名データ４０７が前記図８に示すようにタグなどによって関連付けられている場合には，アプリケーションプログラム２０４ｂ２（情報閲覧者１３０）は，情報生成者１１０から受け取ったデータが生成者署名データ４０７であるかどうかをすぐには判断できない。しかし，後者の場合においても，アプリケーションプログラム２０４ｂ２が，受け取った画像ファイルを真正性保証プログラム２０４ｃを用いて必ず検証するようにすれば，その結果を見ることによって，該データが生成者署名データ４０７であるかどうかを判断することができる。生成者署名データ４０７ではなく単なるマークならば誰も保証していないものであるということを明示するようにしてもよい。

【００８７】また，前記図８のＨＴＭＬファイル内の画像データに付されるタグを，当該画像データが生成者署名データ４０７であることを示すための専用タグとしてもよい。ただし，そのような場合には，あらかじめアプリケーションプログラム２０４ｂ２を，該専用タグが付けられた画像データを受け取った場合に，当該画像データを真正性保証プログラム２０４ｃに渡して処理させるように設定しておくことが必要となる。

【００８８】次に，真正性保証プログラム２０４ｃは，上記生成者署名データ４０７を元データ４００と生成者マーク４０６とに分離し，（生成者署名データの分離３０５），該元データ４００を上記所定の圧縮関数を使って圧縮して圧縮子５００を生成する。

【００８９】上記分離方法は，前述の図４における「生成者署名データの生成３０２」に対応した方法を用いる。たとえば，前記図７に示す方法によって生成者署名データ４０７を生成した場合は，真正性保証プログラム２０４ｃは，図１２に示す処理を行う。

【００９０】図１２において，真正性保証プログラム２０４ｃは，まず，生成者署名データ４０７の中のヘッダ情報を読み取る（ステップ１２００）。そして，該ヘッダ情報の内容にしたがって，生成者署名データ４０７をヘッダ情報と元データ，および生成者マークに分離する（ステップ１２０１）。上記手順において，ヘッダ情報から必要な情報が読み取れないなど，何らかのエラーが

発生した場合には，その旨を情報閲覧者１３０に通知して処理を終了する。

【００９１】一方，前記図８に示すように二つのデータをタグなどによって単に関連付けて，生成者署名データ４０７を生成した場合には，生成者署名データ４０７を元データ４００と生成者マーク４０６とに分離する処理は行わない。

【００９２】再び，図５を参照して情報閲覧者１３０側の処理の詳細を説明する。

【００９３】真正性保証プログラム２０４ｃは，次に，該生成者マーク４０６から情報生成者１１０のディジタル署名４０４を抽出し（生成者ディジタル署名の抽出５０１），さらに，上記圧縮子５００と情報生成者１１０の公開鍵５０２を使って，該ディジタル署名４０４が確かに情報生成者１１０が生成したものであるか否かを検証する（ディジタル署名の検証５０３）。上記処理を適正に行うために，情報閲覧者１３０は，情報生成者１１０の公開鍵５０２をあらかじめ入手しておくか，この時点で入手するものとする。入手方法としては，あらかじめ情報生成者１１０に会って，直接入手する方法が考えられる。しかし，本発明自体は，上記入手方法に限定されるものでなく，たとえば，「ＳＥＣＵＲＥ　ＥＬＥＣＴＲＯＮＩＣ　ＣＯＭＭＥＲＣＥ（著者：Ｗａｒｗｉｃｋ　Ｆｏｒｄ，ＭｉｃｈａｅｌＳ．　Ｂａｕｍ，発行書：Ｐｒｅｎｔｉｃｅ　Ｈａｌｌ　ＰＴＲ）」の１９３ページから２６１ページに記載されているような認証機関（Ｃｅｒｔｉｆｉｃａｔｉｏｎ　Ａｕｔｈｏｒｉｔｙ）と電子認証書（Ｐｕｂｌｉｃ　Ｋｅｙ　Ｃｅｒｔｉｆｉｃａｔｅ）を利用してもよい。すなわち、電子認証書は公開鍵をも含むので、この電子証明書の入手によって公開鍵を入手することができる。

【００９４】電子認証書を入手する方法としては，情報閲覧者１３０が認証機関から情報生成者１１０の電子認証書を直接入手する方法や，前記図４で生成者マーク４０６を生成する際にディジタル署名４０４と画像データ４０５に加えて情報生成者１１０の電子認証書も併せて一纏めにしておき，真正性保証プログラム２０４ｃが生成者マーク４０６から情報生成者１１０のディジタル署名４０４を抽出する際に併せて情報生成者１１０の電子認証書を抽出する方法などがある。

【００９５】次に，真正性保証プログラム２０４ｃは，上記検証結果を表示装置１４１に表示する（検証結果の表示３０７）。該表示は，情報生成者１１０が指定した画像データ４０５と検証の結果とから成り，たとえば，図１のようなものである。すなわち，上記検証において，ディジタル署名１４０が正しく検証できれば，元データ４００が真正なものであると表示する。また，正しく検証できなければ，元データ４００は真正なものではないと表示する。さらに，生成者マーク４０６の中にディジタル署名４０４が含まれておらず，検証処理が実行できなかった場合には，その旨を表示する。情報閲覧者１３０は，これら表示を見ることによって元データ４００が真正なものであるか否かを判断することができる。

【００９６】次に，真正性保証プログラム２０４ｃは，上記元データ４００をアプリケーションプログラム２０４ｂ１に渡す。該二つのプログラム間での元データ４００の受け渡し方法としては，真正性保証プログラム２０４ｃが元データ４００をファイルとして記憶装置に書き込み，アプリケーションプログラム２０４ｂ１が該記憶装置から読み取るといった方法が考えられる。しかし，本発明自体は，上記方法に限定されるものではなく，メモリを介して受け渡してもよい。

【００９７】最後に，アプリケーションプログラム２０４ｂ１は，元データ４００を表示装置１４１に表示する（元データの表示３０８）。該表示に関しては，真正性保証プログラム２０４ｃが，元データ４００のファイル名（拡張子）などから起動すべきアプリケーションプログラムを確認し，アプリケーションプログラム２０４ｂ１に元データ４００を渡すとともに該アプリケーションプログラム２０４ｂ１を起動することによって，自動的に表示するようにすると便利である。

【００９８】上記手順は，ステップ３０７と，ステップ３０８の処理順序を限定するものではない。

【００９９】また，上記手順において，図９に示すように，元データ４００と画像データ（検証結果を含む）との表示処理を，アプリケーションプログラムと真正性保証プログラムとが，それぞれ別々に行っている。しかし，本発明は，上記方法に限定されるものではない。アプリケーションプログラムが画像データも表示可能である場合には，図１０に示すように，元データと画像データとを該アプリケーションプログラムによって表示してもよい。その場合には，真正性保証プログラム２０４ｃは，元データだけでなく画像データをもアプリケーションプログラムに渡す。ただし，アプリケーションプログラムが，画像データを表示する場合でも，前記真正性保証プログラムは，画像データと検証結果との表示を行う。

【０１００】上記の本実施形態では，情報生成者１１０は，任意のアプリケーションプログラムを使って生成した元データ４００に対し，該元データ４００の真正性を保証するディジタル署名４０４を生成した後，画像データ４０５とまとめて生成者マーク４０６を生成するようにしている。そして，該生成者マーク４０６と元データ４００とをまとめて情報閲覧者１３０に渡すようにしている。

【０１０１】また，情報閲覧者１３０は，受け取った生成者マーク４０６に含まれる情報生成者１１０のディジタル署名４０４を用いて，併せて受け取った元データ４００の真正性を検証するようにしている。さらに，該検証結果が視覚，聴覚などによって情報閲覧者１３０に伝

えられるようにしている。

【０１０２】したがって，本発明によれば，不正者が元データ４００を改ざんしたり，生成者マーク４０６を別の情報に付けかえたりした場合には，ディジタル署名４０４の検証処理でエラーとなり，それが視覚，聴覚などで情報閲覧者１３０に伝えられる。結果として，情報閲覧者１３０は，元データ４００が真正なものであるか否かを正しく確認することができる。

【０１０３】次に，本発明の他の実施形態が適用された認証システムの動作について説明する。

【０１０４】図６は，情報生成者１１０が生成した元データに対して，情報認証者１２０が該元データの真正性を保証する認証者署名データを生成し，さらに情報閲覧者１３０が該認証者署名データを用いて元データの真正性を検証する場合の，情報生成者１１０と情報認証者１２０，および情報閲覧者１３０の動作を説明するための図である。

【０１０５】図６において，情報生成者１１０が行う処理には端末１４０_1が使用され，情報認証者１２０が行う処理には端末１４０_2が使用される。また，情報閲覧者１３０が行う処理には端末１４０_3が使用される。

【０１０６】まず，情報生成者１１０は，アプリケーションプログラムを使って情報閲覧者１３０に伝達する元データを生成する（ステップ６００）。そして，該元データを情報認証者１２０に送信する（ステップ６０１）。

【０１０７】元データを受け取った情報認証者１２０は（ステップ６０２），該元データの真正性を保証する認証者マークを生成し（ステップ６０３），当該元データと認証者マークとから認証者署名データを生成する（ステップ６０４）。そして，該認証者署名データを情報生成者１１０に返送する（ステップ６０５）。

【０１０８】情報生成者１１０は，情報認証者１２０から返送されてきた認証者署名データを（ステップ６０６）情報閲覧者１３０に送信する（ステップ６０７）。

【０１０９】認証者署名データを受け取った情報閲覧者１３０は（ステップ６０８），該認証者署名データを元データと認証者マークとに分離し（ステップ６０９），該認証者マークが確かに情報認証者１１０によって生成されたものであるか否かを検証する（ステップ６１０）。そして，該検証結果を確認するとともに（ステップ６１１），元データを適切なアプリケーションプログラムによって確認し（ステップ６１２），全ての処理を終了する。

【０１１０】上記手順において，認証者マークの生成処理(ステップ６０３)，および認証者署名データの生成処理(ステップ６０４)は，図４に示す生成者マークの生成処理(ステップ３０１)，および生成者署名データの生成処理(ステップ３０２)と基本的に同じである。また，認証者署名データの分離処理(ステップ６０９)，認証者マークの検証処理(ステップ６１０)，および検証結果・元データの確認処理(ステップ６１１，６１２)については，図５に示す生成者署名データの分離処理（ステップ３０５），生成者マークの検証処理(ステップ３０６)，および検証結果・元データの確認処理(ステップ３０７，３０８)と基本的に同じである。その他，図６における，ステップ６００，６０７，６０８は，それぞれ，図３のステップ３００，３０３，３０４に相当する。

【０１１１】また，上記手順では，情報生成者１１０から情報認証者１２０に対して元データを送っているが，情報生成者１１０側で元データの圧縮子を生成し，該圧縮子を情報認証者に送るようにしてもよい。この場合は，元データの内容が，情報認証者にはわからないようにすることができる。

【０１１２】上記の本実施形態では，情報認証者１２０は，情報生成者１１０が任意のアプリケーションプログラムを使って生成した元データの真正性を保証するディジタル署名を生成した後，画像データと一纏めにして認証者マークを生成するようにしている。そして，該認証者マークと元データとを一纏めにして情報生成者１１０に渡すようにしている。

【０１１３】また，情報生成者１１０は，情報認証者１２０から返送された認証者マークと元データを情報閲覧者１３０に渡すようにしている。

【０１１４】さらに，情報閲覧者１３０は，受け取った認証者マークに含まれる情報認証者１２０のディジタル署名を用いて，併せて受け取った元データの真正性を検証するようにしている。加えて，該検証結果が視覚，聴覚などによって情報閲覧者１３０に伝えられるようにしている。

【０１１５】したがって，本発明によれば，不正者が元データを改ざんしたり，認証者マークを別の情報に付けかえたりした場合には，ディジタル署名の検証処理でエラーとなり，それが視覚，聴覚などで情報閲覧者１３０に伝えられる。結果として，情報閲覧者１３０は，元データが真正なものであるか否かを正しく確認することができる。

【０１１６】なお，本発明は，上記各実施例に限定されるものではなく，その要旨の範囲内で様々な変形が可能である。

【０１１７】たとえば，本発明では，検証結果の如何に依らず元データを表示するようにしているが，本発明はこれに限定されない。検証の結果，元データの真正性が確認された場合に，適切なアプリケーションプログラムを使って元データを表示するようにしてもよい。この場合は，図５において，ステップ３０７の結果によって，ステップ３０８の処理が制御されることになる。

【０１１８】また，本発明では，真正性保証プログラムが生成者署名データを受け取った場合に自動的に検証処理を行うようにしているが，本発明はこれに限定されな

い。情報閲覧者が明示的に指示を出したときに行うようにしてもよい。そのような場合，真正性保証プログラムは，生成者マークの代わりに，検証処理が済んでいない生成者マークがあることを示すための独自の画像データを表示するようにすると，情報閲覧者にわかりやすく便利である。

【０１１９】さらに，上記各実施例では，画像データとディジタル署名とを一纏めにする場合について説明しているが，文字データ，画像データ，ビデオデータ，音データなどのマルチメディア，さらにはこれらを組み合わせたマルチメディアデータにも適用可能であることは自明である。

【０１２０】加えて，上記各実施例では，元データ（または，元データの圧縮子）をディジタル署名の対象としているが，本発明はこれに限定されない。たとえば，該元データの有効期限や，原本，謄本の区別などといった属性情報を生成し，該属性情報と元データとをディジタル署名の対象としてもよい。

【０１２１】例えば，元データがある期間内だけ有効であり，それを過ぎると効力を失うようなものであった場合，元データと生成者マーク（認証者マーク），ならびに有効期限から生成者署名データ（認証者署名データ）を生成し，検証結果を情報閲覧者に伝える際に有効期限も併せて伝えるようにしてもよい。

【０１２２】また，原本の保管場所（物理的な場所（例えば住所）と論理的な場所（例えばURL）のどちらでもよい）を生成者署名データ（認証者署名データ）の生成要素の一つとし，検証の際に、上記保管場所の情報を用いて、当該閲覧データが原本であるか謄本であるかを判断し、署名検証結果を情報閲覧者に伝える際に，その判断結果を併せて伝えるようにしてもよい。

【０１２３】また，元データに対するアクセス制御情報を属性情報に含めることもできる。アクセス制御情報を含めた場合，真正性保証プログラムは，当該アクセス制御情報を参照して情報閲覧者が当該元データを見る権利があるかどうかを判断し，権利がある場合にアプリケーションプログラムに元データを渡すようにする。この場合，さらに，元データを情報生成者側で暗号化し，情報閲覧者に見る権利がある場合に復号するようにしてもよい。

【０１２４】さらに，本発明では，情報閲覧者の端末で真正性の検証処理を行っているが，本発明はこれに限定されない。たとえば，情報生成者がインターネットのようなオープンなネットワーク上で公開している情報（生成者署名データ）を，あるポリシーによって管理されているドメイン内（例えば，企業や学校など）の情報閲覧者が見る場合に，当該ドメインのドメイン内ネットワークとインターネットとの間に設置されているファイアウォール等のゲートウェイ装置で真正性の検証処理を行ってもよい。その場合，さらに，真正性が確認されない情報はドメイン内ネットワークに流さないようにしたり，特定のマークが付加されている情報以外はドメイン内ネットワークに流さないようにしたりすると，安全性や利便性が高まる。

【０１２５】また，上記各実施例の各端末に格納された各プログラムは，一般的には，それぞれの装置を制御するオペレーティングシステムの元で動作し，オペレーティングシステムを介して，装置の各ハードウェア構成要素とデータ，コマンドをやり取りする。もちろん，オペレーティングシステムを介さずに直接，各ハードウェア構成要素とデータ，コマンドのやり取りをしてもよい。

【０１２６】加えて，これらのプログラムが各端末に格納される際に，フロッピーディスク，ＣＤ－ＲＯＭ，ＤＶＤ等各種記憶媒体に格納された形態で供給されるか，あるいはこれらの端末が接続されたネットワークに接続された他の端末からダウンロードされることがある。

【０１２７】さらに加えて，本発明では，通信網１００を流れるデータを暗号化してはいないが，情報の機密性を保証するために別途暗号通信を行ってもよい。

【０１２８】以上説明したように，本発明によれば，第一のユーザが生成したマルチメディアデータの真正性を，第二のユーザが視覚，聴覚などによって正しく確認することができる。

【０１２９】

【発明の効果】以上説明したように，本発明によれば，第一のユーザが生成したマルチメディアデータが真正なものであるか否かを，そのマルチメディアデータのフォーマットやそれを処理するアプリケーションプログラムに依らず，第二のユーザが視覚，聴覚などで直接的に確認することができるので，安全性を確保することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施形態が適用された認証システムの概略構成を示す図である。

【図２】図１に示す端末のハードウェア構成を示す図である。

【図３】本発明の第１の実施形態が適用された認証システムにおいて，情報生成者が生成した元データの真正性を情報閲覧者が検証する際の動作を説明するためのフロー図である。

【図４】図３に示す情報生成者の処理の詳細を示す図である。

【図５】図３に示す情報閲覧者の処理の詳細を示す図である。

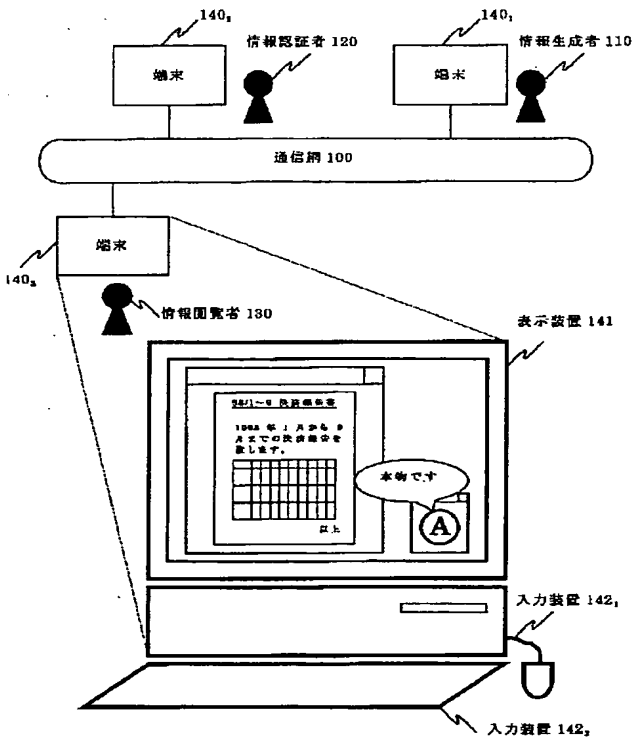
【図６】本発明の他の実施形態が適用された認証システムにおいて，情報生成者が生成した元データの真正性を情報認証者が保証するとともに，該真正性を情報閲覧者が検証する際の動作を説明するためのフロー図である。

【図７】生成者マークと元データとを一纏めにする方法の一例を示す図である。

【図８】生成者マークと元データとを一纏めにする方法の別の例を示す図である。
【図９】元データと画像データ，および検証結果を表示する方法の一例を示す図である。
【図１０】元データと画像データ，および検証結果を表示する方法の別の例を示す図である。
【図１１】元データと生成者マークとを生成者署名データに纏める際の真正性保証プログラムの処理の流れの一例を示すフロー図である。
【図１２】生成者署名データを元データと生成者マークとに分離する際の真正性保証プログラムの処理の流れの一例を示すフロー図である。
【符号の説明】
１００：通信網
１１０：情報生成者
１２０：情報認証者
１３０：情報閲覧者
１４０（140_1～140_3）：端末
１４１：表示装置
１４２：入力装置
２００：バス
２０１：通信網インターフェース
２０２：記憶装置
２０３：ＣＰＵ
２０４：メモリ
２０４ａ：オペレーティングシステム
２０４ｂ：アプリケーションプログラム
２０４ｃ：真正性保証プログラム

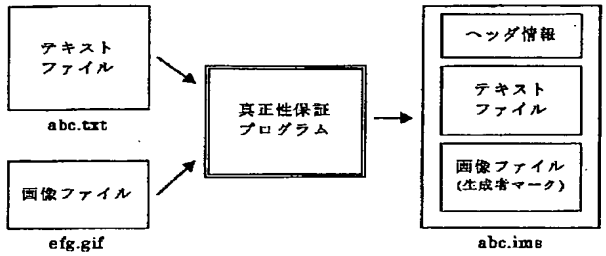
【図１】

図１



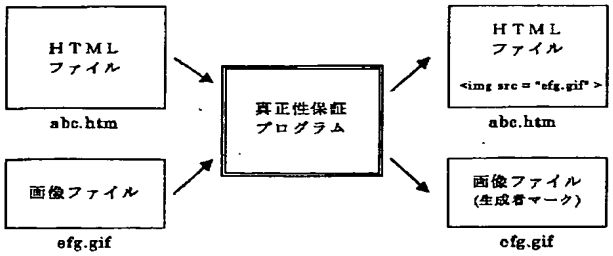
【図７】

図７



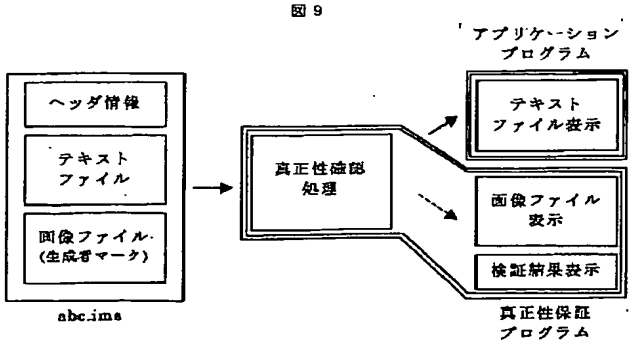
【図８】

図８



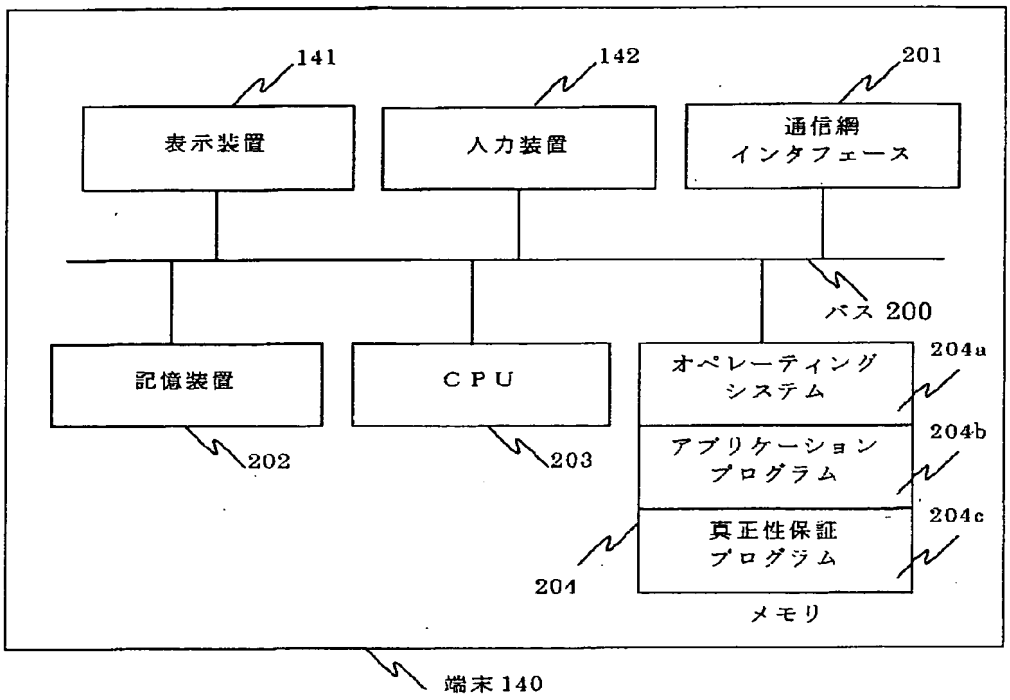
【図９】

図９



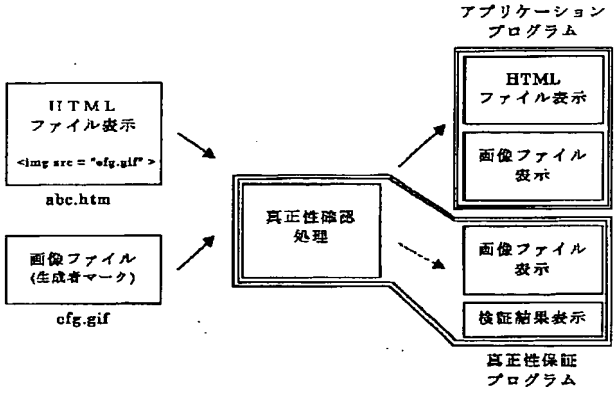
【図２】

図２



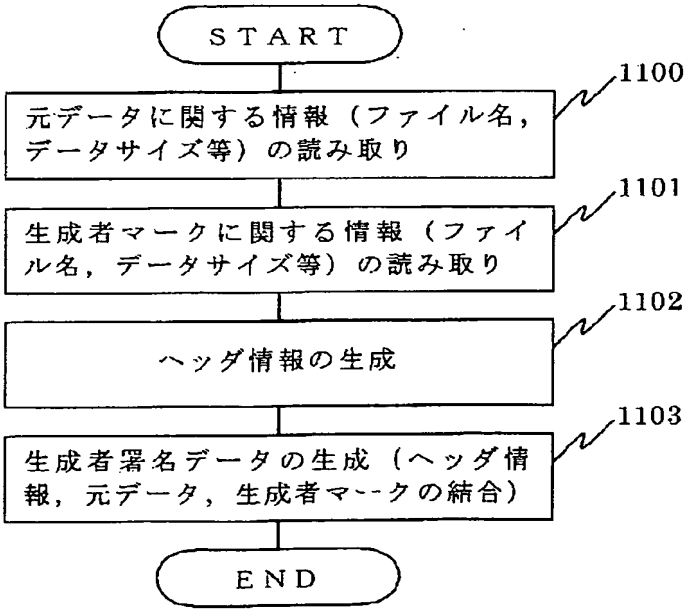
【図１０】

図１０



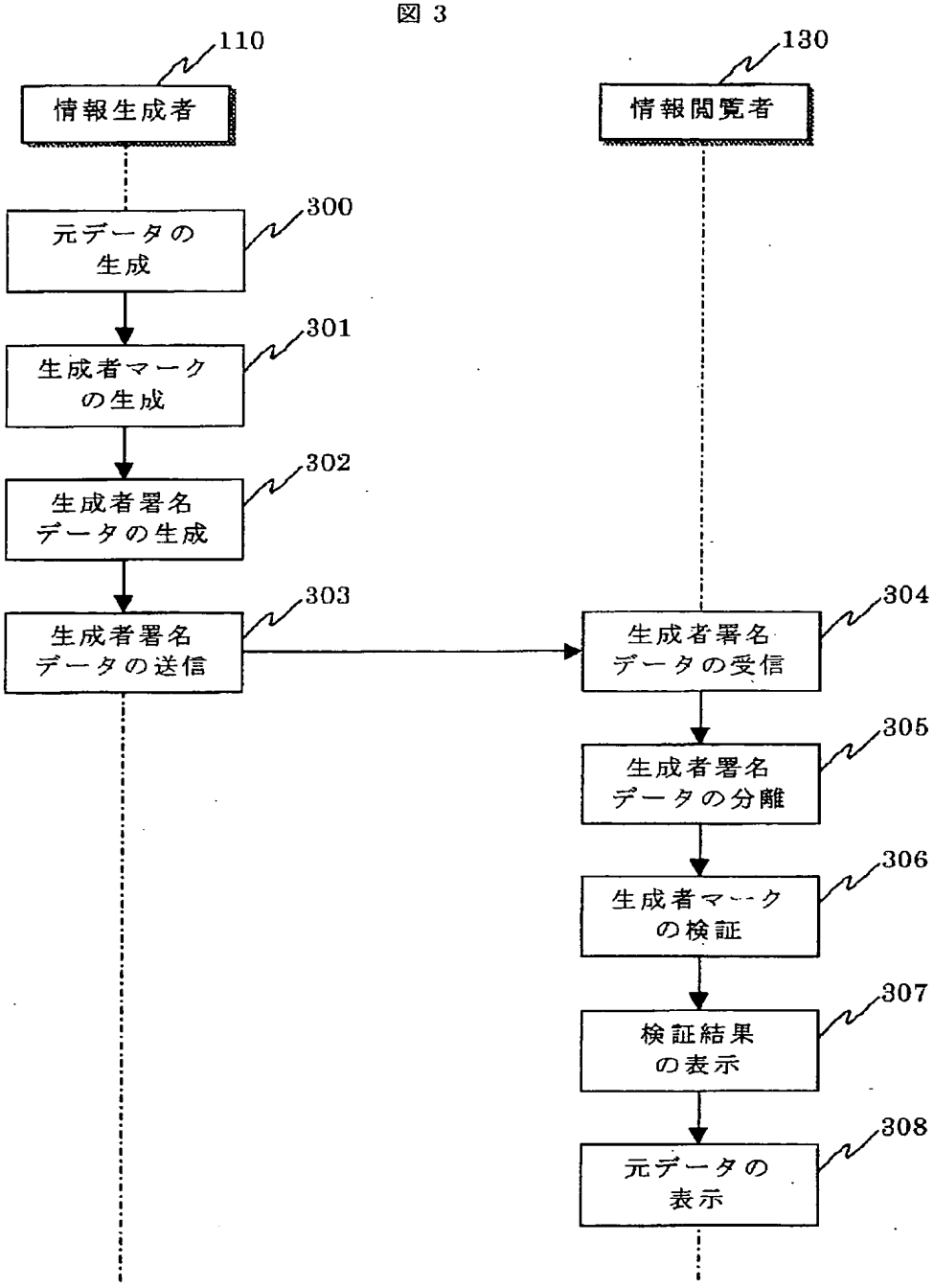
【図１１】

図１１



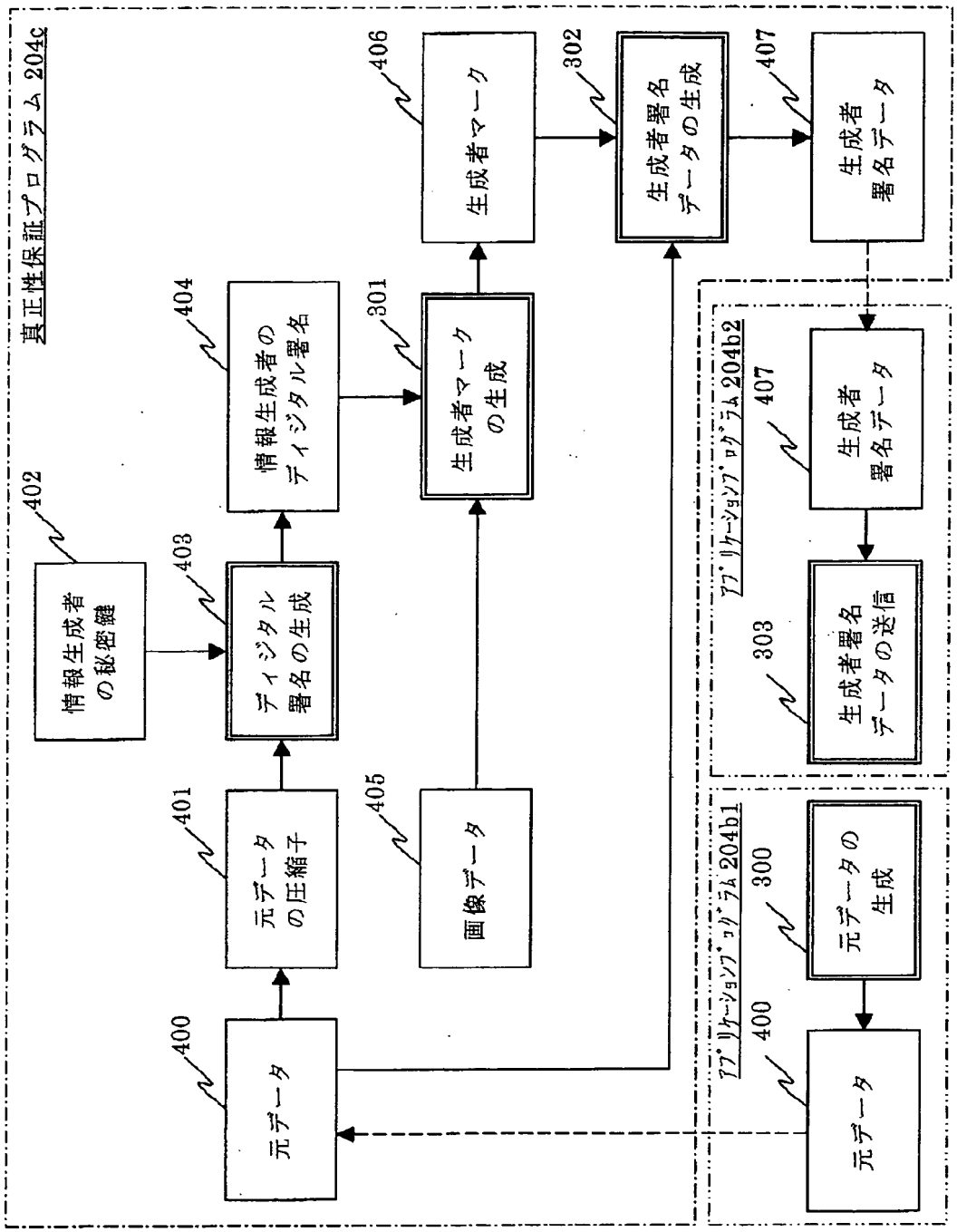
【図３】

図 3


110
情報生成者
130
情報閲覧者
300
元データの生成
301
生成者マークの生成
302
生成者署名データの生成
303
生成者署名データの送信
304
生成者署名データの受信
305
生成者署名データの分離
306
生成者マークの検証
307
検証結果の表示
308
元データの表示

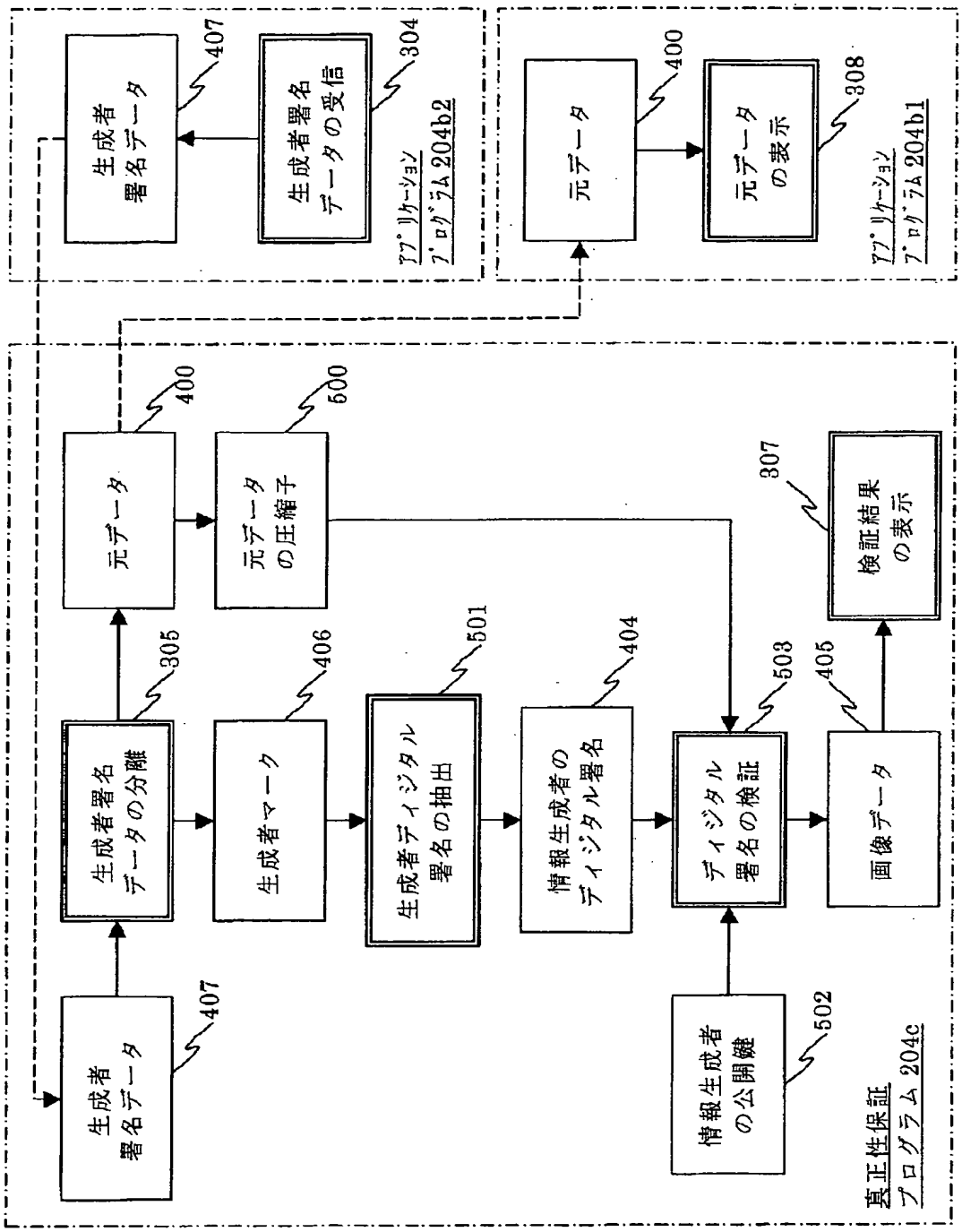
【図４】

図 4


真正性保証プログラム 204c
情報生成者の秘密鍵
402
ディジタル署名の生成
403
情報生成者のディジタル署名
404
生成者マークの生成
301
生成者マーク
406
生成者署名データの生成
302
生成者署名データ
407
元データの圧縮子
401
画像データ
405
元データ
400
アプリケーションプログラム 204b2
生成者署名データ
407
生成者署名データの送信
303
アプリケーションプログラム 204b1
元データの生成
300
元データ
400

【図５】

図 5


生成者署名データ
407
生成者署名データの受信
304
アプリケーションプログラム 204b2
元データ
400
元データの表示
308
アプリケーションプログラム 204b1
元データ
400
元データの圧縮子
600
検証結果の表示
307
生成者署名データの分離
305
生成者マーク
406
生成者ディジタル署名の抽出
501
情報生成者のディジタル署名
404
ディジタル署名の検証
503
画像データ
405
生成者署名データ
407
情報生成者の公開鍵
502
真正性保証プログラム 204c

【図６】

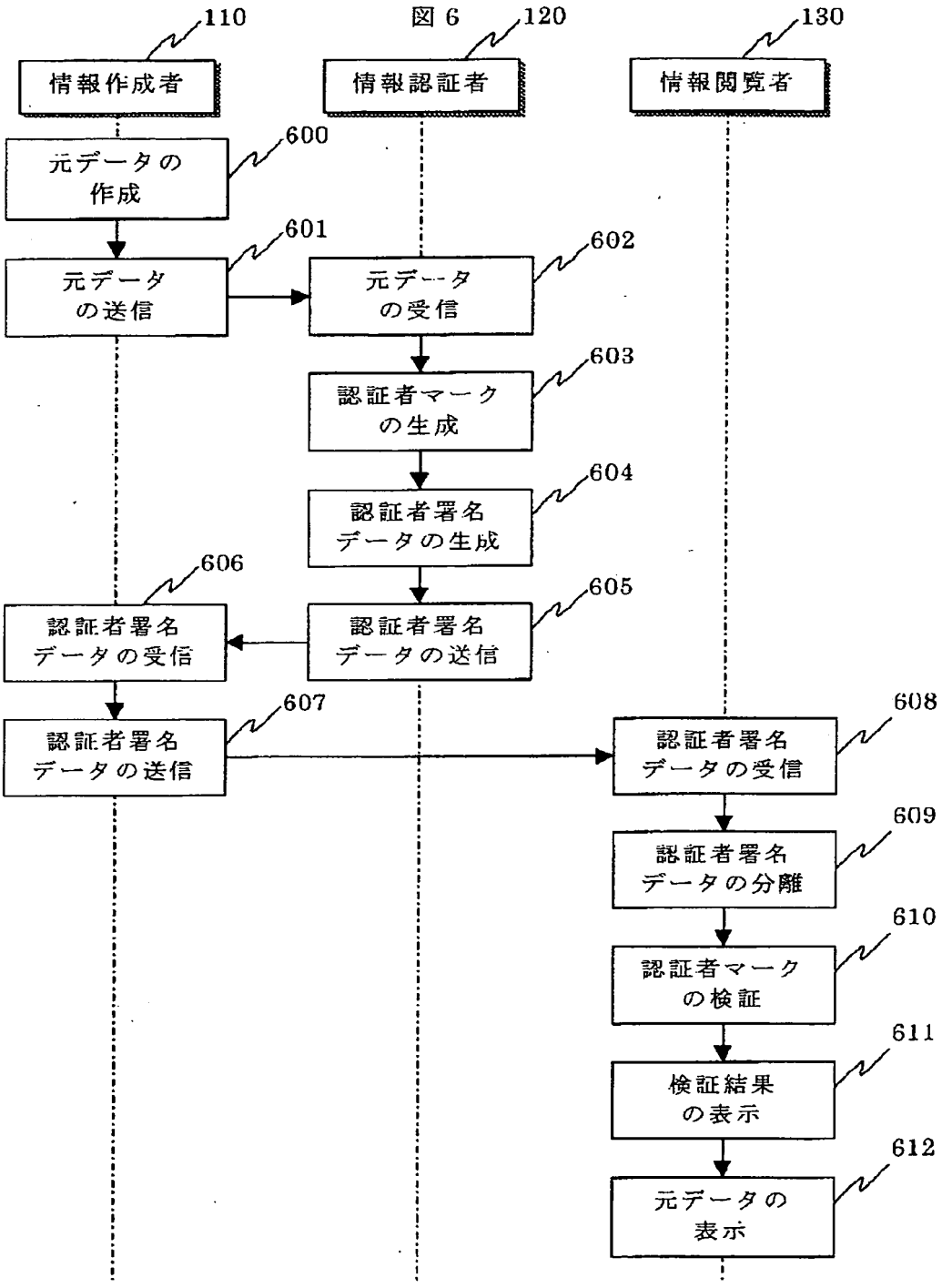
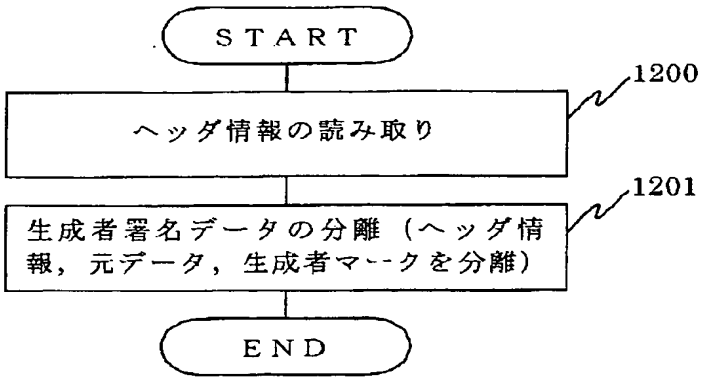


図 6
110
120
130
情報作成者
情報認証者
情報閲覧者
600
元データの作成
601
元データの送信
602
元データの受信
603
認証者マークの生成
604
認証者署名データの生成
605
認証者署名データの送信
606
認証者署名データの受信
607
認証者署名データの送信
608
認証者署名データの受信
609
認証者署名データの分離
610
認証者マークの検証
611
検証結果の表示
612
元データの表示

【図１２】

図１２



フロントページの続き

(51) Int. Cl.[7]	識別記号	Ｆ Ｉ	ﾃｰﾏｺｰﾄﾞ（参考）
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ｂ

(72)発明者　長野　裕美
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共情報事業部内

(72)発明者　豊田　英樹
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア事業部内

(72)発明者　鍛　忠司
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内